## R E M A R K S

Careful review and examination of the subject application are noted and appreciated.

## SUPPORT FOR THE CLAIM AMENDMENTS

Support for the claim amendments may be found in the specification, for example, on page 7 lines 2-13, page 28 liens 3-11, page 23 lines 11-18, page 28 line 17-page 29 line 2, and FIGS. 1, 7 and 9, as originally filed. Thus, no new matter has been added.

## CLAIM REJECTIONS UNDER 35 U.S.C. §101

The rejection of claims 1-10 under 35 U.S.C. §101 has been obviated by appropriate amendment and should be withdrawn.

Claims 1-10 have been directed to a method for a circuit in the electronic technology art. As such, claims 1-10 are directed to a statutory subject matter and the rejection should be withdrawn.

## CLAIM REJECTIONS UNDER 35 U.S.C. §102

The rejection of claims 1, 2, 7-12 and 17-20 under 35 U.S.C. §102(b) as being anticipated by Ritter '549 has been obviated by appropriate amendment and should be withdrawn.

Ritter concerns a cipher mechanism with fencing and balanced block mixing (Title).

Claim 1 provides steps for (A) copying a plurality of symbols from a source file to a plurality of tables of a circuit and (C) generating a plurality of block output signals each responsive to (i) one of a plurality of block input signals and (ii) the symbols in one of the tables. In contrast, Ritter appears to be silent regarding copying a plurality of symbols from a source file to a plurality of substitution mechanisms 182 (asserted to generate the claimed block output signals). Therefore, Ritter does not appear to disclose or suggest steps for (A) copying a plurality of symbols from a source file to a plurality of tables of a circuit and (C) generating a plurality of block output signals each responsive to (i) one of a plurality of block input signals and (ii) the symbols in one of the tables as presently claimed. Claims 11 and 20 provide language similar to claim 1. As such, claims 1, 11 and 20 are fully patentable over the cited reference and the rejection should be withdrawn.

Claim 2 provides a step for permutating each of a plurality of portions of an intermediate result to present an output signal. Despite the assertion on page 4 of the Office Action, blocks 182 in FIG. 10 of Ritter and the text in column 16, line 66 through column 17, line 8 of Ritter appear to be silent regarding **permutating**. Therefore, Ritter does not appear to

disclose or suggest a step for permutating each of a plurality of portions of an intermediate result to present an output signal as presently claimed. Claim 12 provides language similar to claim 2. As such, claims 2 and 12 are fully patentable over the cited reference and the rejection should be withdrawn.

Claim 8 provides that fewer than a predetermined number of units of an input signal are allocated to one of a plurality of block input signals. In contrast, Ritter appears to be silent regarding any allocation other than k bits **to each** of the signals entering one of the substitution mechanisms 182 (asserted to receive the claimed block input signals). Therefore, Ritter does not appear to disclose or suggest that fewer than a predetermined number of units of an input signal are allocated to one of a plurality of block input signals as presently claimed. Furthermore, the Office Action makes no arguments regarding the language of claims 8 and 18. In particular, the arguments on pages 4 and 5 of the Office Action appear to be limited to claims 7 and 17. Therefore, *prima facie* anticipation has not been established. Claim 18 provides language similar to claim 8. As such, the rejection of claims 8 and 18 should be withdrawn.

Claim 9 provides a step for generating an input signal by counting a clock signal. In contrast, Ritter appears to be silent regarding **counting clock signals**. Therefore, Ritter does not appear to disclose or suggest a step for generating an input signal

by counting a clock signal as presently claimed. Claim 19 provides language similar to claim 9. As such, claims 9 and 19 are fully patentable over the cited reference and the rejection should be withdrawn.

Claim 10 provides a step for generating a plurality of the output signals in response to a plurality of the countings. Despite the assertion on page 5 of the Office Action, Ritter appears to be silent regarding any counting, let alone a plurality of countings. Therefore, Ritter does not appear to disclose or suggest a step for generating a plurality of output signals in response to a plurality of countings as presently claimed. As such, claim 10 is fully patentable over the cited reference and the rejection should be withdrawn.

**CLAIM REJECTIONS UNDER 35 U.S.C. §103**

The rejection of claims 3-6 and 13-16 under 35 U.S.C. §103(a) as being unpatentable over Ritter in view of Sprunk '693 has been obviated by appropriate amendment and should be withdrawn.

Ritter concerns a cipher mechanism with fencing and balanced block mixing (Title). Sprunk concerns an apparatus for avoiding complementarity in an encryption algorithm (Title).

Claim 3 provides that each table comprises k columns and 2^k rows, where k is a bit width of each of the block input signals and each of the rows store **a unique one** of the plurality of

symbols. In contrast, an S-Box S1 table in column 4 of Sprunk appears to show that each number in the table (asserted similar to the claims symbols) is repeated multiple times. Therefore, Ritter and Sprunk, alone or in combination, do not appear to teach or suggest a table comprising k columns and 2^k rows, where k is a bit width of each of a block input signal and each of the rows stores a unique one of a plurality of symbols as presently claimed. Claim 13 provides language similar to claim 3. As such, claims 3 and 13 are fully patentable over the cited references and the rejection should be withdraw.

Claim 4 provides that each of the plurality of symbols in the source file have an approximately equal probability of appearance. In contrast, both Ritter and Sprunk appear to be silent regarding (i) **a source file** from which the symbols are extracted or (ii) any probability of the symbols in the source file. Therefore, Sprunk and Ritter, alone or in combination, do not appear to teach or suggest that each of a plurality of symbols in a source file has an approximately equal probability of appearance as presently claimed. Claim 14 provides language similar to claim 4. As such, claims 4 and 14 are fully patentable over the cited references and the rejection should be withdrawn.

Claim 5 provides a step for selecting a starting point within the source file to extract the symbols for a first table of a plurality of tables. In contrast, both Ritter and Sprunk appear

to be silent regarding a source file for the symbols. Therefore, Ritter and Sprunk, alone or in combination, do not appear to teach or suggest a step of selecting a starting point within a source file to extract symbols for a first table of a plurality of tables as presently claimed.

Claim 5 further provides a step for calculating a number of symbols extracted for the first table. In contrast, both Ritter and Sprunk appear to be silent regarding calculating a number of symbols extracted from the unidentified source file. Therefore, Ritter and Sprunk, alone or in combination, do not appear to teach or suggest a step toward calculating a number of symbols extracted for a first table as presently claimed.

Claim 5 further provides a step for calculating a subsequent starting point to extract the symbols for a subsequent table of the plurality of tables based upon the starting point and the number. In contrast, both Ritter and Sprunk appear to be silent regarding calculation of a subsequent starting point as presently claimed. Claim 15 provides language similar to claim 5. As such, claims 5 and 15 are fully patentable over the cited references and the rejection should be withdrawn.

Claim 6 provides a step of presenting both a bit width of the block signals and a starting point external to the circuit as a cryptographic key. In contrast, both Ritter and Sprunk appear to be silent regarding a **presentation** of a cryptographic key external

to a circuit wherein the cryptographic key includes both a bit width and a starting point in a source file. Therefore, Ritter and Sprunk, alone or in combination, do not appear to teach or suggest a step for presenting both a bit width of a plurality of block signals and a starting point external to a circuit as a cryptographic key as presently claimed. Claim 16 provides language similar to claim 6. As such, claims 6 and 16 are fully patentable over the cited references and the rejection should be withdrawn.

Dependent claims 7 and 17 depend from independent claims 1 and 11, which are now believed to be allowable. Since the dependent claims contain all the limitations of the independent claims, claims 7 and 17 are fully patentable over the cited references and the rejection should be withdrawn.

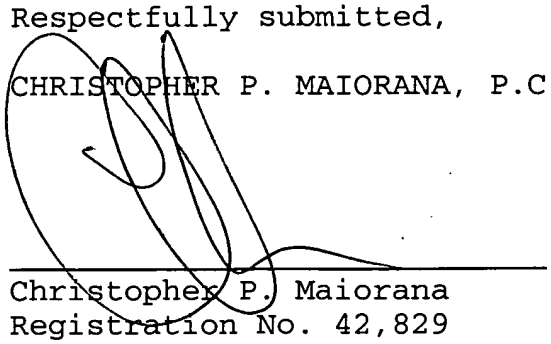
Accordingly, the present application is in condition for allowance. Early and favorable action by the Examiner is respectfully solicited.

The Examiner is respectfully invited to call the Applicants' representative at 586-498-0670 should it be deemed beneficial to further advance prosecution of the application.

If any additional fees are due, please charge Deposit Account No. 12-2252.

Respectfully submitted,

CHRISTOPHER P. MAIORANA, P.C.



Christopher P. Maiorana
Registration No. 42,829

Dated: May 23, 2005

c/o Timothy Croll
LSI Logic Corporation
1621 Barber Lane, M/S D-106 Legal
Milpitas, CA 95035

Docket No.: 01-308 / 1496.00129